ABSTRACT OF THE DISCLOSURE

The present invention presents a public key cryptographic system and method called Absolute Public Key Cryptography that survives private key compromise and offers two-way communication security. Communications are secured even when the private key is revealed. It provides security to the private-to-public side communications and also allows short keys to be used with mobile devices that have low processing power. The system uses keys with two or more components and encrypts a message into the same number of cipher versions. The cipher versions are delivered to the destination in source routing mode, or hop-by-hop routing mode with a small time gap. The recipient performs certain mathematical operations on all the cipher versions and obtains the original message. All the versions are necessary for obtaining the original message. Even a single version missing leads to produce a junk for an attacker. As an attacker at an intermediary IP router can not have all the cipher versions available, he can not obtain the original message even when he knows the private key. This is why the system is called Absolute Public Key Cryptography. The robustness against private key compromise is achieved by blinding the public key through adding a random number to each of its components before encryption. When the encryption process is complete, the random number is discarded and the cipher versions are delivered to the recipient. The effect of blinding is made void by the actual intended recipient, who has all the cipher versions available. Robustness is also achieved another way, that is, by choosing the encrypting key such that each of its components has a common factor with Euler Totient Function of the key modulus, and there is no common factor among all the components. This makes it harder for an attacker to decrypt a single cipher version of the message into the original message and thereby allows smaller keys to be used for mobile communications. Communication in both directions is secured by using two different key pairs, one for public-to-private-side and the other for private-to-public-side communications.